§170.315(d)(9) Trusted connection

2015 Edition CCGs

Version 1.3 Updated on 09-29-2017

Revision History

Version #	Description of Change	Version Date
1.0	Initial Publication	10-30-2015
1.1	Clarification added on what must be demonstrated during testing of the trusted connection for transport.	01-29-2016
1.2	Clarification added for transport level encryption.	05-26-2017
1.3	Updated to reference 'HTTPS' in paragraph (d)(9)(ii).	09-29-2017

Regulation Text

Regulation Text

§170.315 (d)(9) *Trusted connection—*

Establish a trusted connection using one of the following methods:

(i) *Message-level.* Encrypt and integrity protect message contents in accordance with the standards specified in §170.210(a)(2) and (c)(2).

(ii) *Transport-level.* Use a trusted connection in accordance with the standards specified in §170.210(a)(2) and (c)(2).

Standard(s) Referenced

Applies to entire criterion

§ 170.210(a)(2) *General.* Any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing

Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, October 8, 2014

§ 170.210(c)(2) A hashing algorithm with a security strength equal to or greater than SHA-2 as specified by NIST in FIPS Publication 180-4, Secure Hash Standard, 180-4 (August 2015)

Certification Companion Guide: Trusted connection

This Certification Companion Guide (CCG) is an informative document designed to assist with health IT product development. The CCG is not a substitute for the 2015 Edition final regulation. It extracts key portions of the rule's preamble and includes subsequent clarifying interpretations. To access the full context of regulatory intent please consult the 2015 Edition final rule or other included regulatory reference. The CCG is for public use and should not be sold or redistributed.

Link to Final Rule Preamble

Edition Comparision	Gap Certification Eligible	Base EHR Definition
New	No	Not Included

Certification Requirements

This certification criterion at § 170.315(d)(9) is required as part of the 2015 Edition privacy & security approach for the certification criteria at § 170.315(e)(1), (e)(2), (e)(3), (g)(7), (g)(8), and (g)(9). This certification criterion at § 170.315(d)(9) must be explicitly demonstrated with § 170.315(e)(1) and (e)(2) because of the specific capabilities for secure electronic transmission and secure electronic messaging included in each of these two criteria, respectively. For the other certification criteria (§ 170.315(e)(3), (g)(7), (g)(8), and (g)(9)), this criterion at § 170.315(d)(9) only needs to be demonstrated once as part of the overall scope of the certificate sought.

Quality management system (§ 170.315(g)(4)) and accessibility-centered design (§ 170.315(g)(5)) must be certified as part of the overall scope of the certificate issued to the product.

- When a single quality management system (QMS) is used, the QMS only needs to be identified once. Otherwise, the QMS' need to be identified for every capability to which it was applied.
- When a single accessibility-centered design standard is used, the standard only needs to be identified once. Otherwise, the accessibility-centered design standards need to be identified for every capability to which they were applied; or, alternatively the developer must state that no accessibility-centered design was used.

Table for Design and Performance

- Quality management system (§ 170.315(g)(4))

- Accessibility-centered design (§ 170.315(g)(5))

Technical Explanations and Clarifications

Applies to entire criterion

Clarifications:

- Health IT needs to provide a level of trusted connection using either 1) encrypted and integrity message protection or 2) a trusted connection for transport. Either of these methods must be demonstrated in accordance with the following standards: Annex A: FIPS Publication 140-2, Security Requirements for Cryptographic Modules and FIPS PUB 180-4, Secure Hash Standard, 180-4.
- A "trusted connection" means the link is encrypted/integrity protected according to § 170.210(a)(2) or (c)(2). As such, we do not believe it is necessary to specifically name HTTPS and/or SSL/TLS as this standard already covers encryption and integrity protection for data in motion. [see also 80 FR 62676]

Paragraph (d)(9)(i)

Technical outcome – The health IT offers a user encrypted and integrity message protection.

Clarifications

- No additional clarifications available.

Paragraph (d)(9)(ii)

Technical outcome – The health IT provides the user a trusted connection for transport.

Clarifications

- The tester is required to view the encryption handshake to ensure that the digital certificates, where used, are being invoked during the connection. Developers have freedom to demonstrate the encryption handshake based on the technology they are using. For example, if a developer has a browser-based module that uses HTTPS, the developer could demonstrate the "lock" icon in the browser that indicates that HTTPS is present and working properly.
- The verification step is verifying that the transport is conducted using a trusted connection configured to conform to the required level of encryption and hashing standard. The communication content is not examined, only the configuration and the handshake, and where used, the digital certificates. The messages are not examined as with alternative 1. The lab does not need to verify the messages, only the trusted connection.

Content last reviewed on June 23, 2020